How explicit are the barriers to failure in safety arguments?

Shamus P. Smith*, Michael D. Harrison**, and Bastiaan A. Schupp

Dependability Interdisciplinary Research Collaboration,
Department of Computer Science,
University of York, York YO10 5DD,
United Kingdom.
{Shamus.Smith, Michael.Harrison, Bastiaan.Schupp}@cs.york.ac.uk

Abstract. Safety cases embody arguments that demonstrate how safety properties of a system are upheld. Such cases implicitly document the barriers that must exist between hazards and vulnerable components of a system. For safety certification, it is the analysis of these barriers that provide confidence in the safety of the system.
The explicit representation of hazard barriers can provide additional insight for the design and evaluation of system safety. They can be identified in a hazard analysis to allow analysts to reflect on particular design choices. Barrier existence in a live system can be mapped to abstract barrier representations to provide both verification of barrier existence and a basis for quantitative measures between the predicted barrier behaviour and performance of the actual barrier. This paper explores the first stage of this process, the binding between explicit mitigation arguments in hazard analysis and the barrier concept. Examples from the domains of computer-assisted detection in mammography and free route airspace feasibility are examined and the implications for system certification are considered.

1 Introduction

Barriers are often complex socio-technical systems: a combination of technical, human and organisational measures that prevent or protect against an adverse effect. Barriers for safety critical systems include physical representations, for example a mechanical guard on an electronic throttle [1], as well as beliefs, such as confidence in system safety based on conformance to applied standards. A no smoking sign is a typical example of a barrier as a complex system. Although the sign aims to prevent fire from cigarettes, it is not just the sign. The barrier includes awareness of how smoking may cause fires, awareness of the significance

* Now at the Department of Computer Science, University of Durham, Durham DH1 3LE, shamus.smith@durham.ac.uk
** Now at the Informatics Research Institute, University of Newcastle Upon Tyne, Newcastle Upon Tyne, NE1 7RU, michael.harrison@ncl.ac.uk

of the sign, the sign's visibility, training of the smokers, and its relation to other barrier systems such as an installed smoke alarm and sprinkler system [19].

Barriers embody both abstract and concrete representations of properties commonly argued in a safety case. Kelly et al. [11] defines a safety case as the document, or set of documents, presenting the argument that a system is acceptably safe to operate in a given context. Such cases implicitly document the barriers that must exist between hazards and hazardous states and vulnerable components of a system. For certification it is the verification of these barriers that provide confidence in the safety of the system. However, explicit representations of such barriers are commonly absent from safety case documentation and the associated arguments for compliance to particular standards.

Explicit barrier description in hazard analysis can provide insight throughout the development of safety critical systems and in addition aid safety certification by documenting barrier development through design to implementation in a live system. For example if there is a hazard mitigation that an interlock[1] inhibits some type of behaviour, this may feature as evidence in a safety case. It should be possible to prove that it is in place in the live system and that its performance can be accessed and compared to predicted performance in the initial hazard analysis.

This paper investigates the binding of explicit mitigation arguments in hazard analysis to the barrier concept. Identifying explicit barriers early in system development can allow informed decision making through design and implementation phases of a system's development. The remainder of this paper is as follows. Section 2 describes barriers in relation to risk reduction in design and implementation. Section 3 presents an overview of barriers in the context of hazard analysis. The use of explicit barriers to highlight hazard and barrier properties are exemplified in two case studies in Sections 4 and 5. Section 6 overviews the use of explicit barriers for certification. Section 7 presents conclusions.

2 Risk reduction and barriers

Risk reduction is a key factor in the design of safety critical systems and in assessment of their operational safety. It is achieved either by preventing hazards or by protecting against hazards. Prevention typically involves design modifications of the total system, including for example operating procedures. Protection involves the design of additional systems, which embody barriers that fend against adverse events, damage or harm [19]. Barriers represent the diverse physical and organisational measures that are taken to prevent a target from being affected by a potential hazard [10, pg 359]. A barrier is an obstacle, an obstruction, or a hindrance that may either (i) prevent an action from being carried out or an event from taking place, or (ii) prevent or lessen the impact of the consequences, limiting the reach of the consequences or weakening them in some way [9].

[1] An interlock is a mechanism which ensures that potentially hazardous actions are only performed at times when they are safe [22].

The concepts and terminology related to barriers or safety features vary considerably [7], for example Hollnagel [9] presents a classification of barrier systems based on four main categories:

1. *Material barriers* physically prevent an action from being carried out or the consequences of a hazard from spreading. For example a fence or wall.
2. *Functional barriers* impede an action from being carried out, for instance the use of an interlock.
3. *Symbolic barriers* require an act of interpretation in order to achieve their purpose. For example a give way sign indicates a driver should give way but does not actively enforce/stop non-compliance.
4. *Immaterial barriers* are not physically present or represented in the situation, but depend on the knowledge of the user to achieve their purpose. For example the use of standards.

This paper makes no commitment to the terminology of barriers and instead focuses on the presence of barriers, in whatever form, in the context of a hazardous event or action. The pre- and post-condition states of a hazard are represented by preventive and protective barriers respectively. Therefore the use of barriers, either for the prevention of hazards or the protection from hazardous effect, is considered to be part of the process of hazard analysis.

3 Hazard analysis and barriers

Hazard analysis is at the heart of any safety programme [13, pg 287]. It is a necessary first step before hazards can be eliminated or controlled through design or operational procedures. Within hazard analysis, descriptive arguments[2] are implicitly used to justify prevention arguments of identified hazards.

Previous work has demonstrated that explicit mitigation arguments allow an analyst to reflect on the mitigations present and constitute an initial step to processes such as argument reuse in hazard analysis [20, 21]. In addition, explicit arguments document the reasoning being applied in an analysis session. If such decisions are lost, evaluation of the analysis and certification can be problematic.

Mitigation arguments to hazards are implicitly described in terms of barriers. Barriers against hazards may take a variety of forms for example procedures, training, human action, as well as, systems and components that prevent accidents or provide mitigation of consequences and constitute barriers against injury [14, pg A-1].

Although a range of methods have been developed to support systematic hazard analysis, for example, HAZOP (Hazard and Operability Studies) [12], FMEA (Failure Modes and Effect Analysis) [3] and THEA (Technique for Human Error Assessment) [15], such methods stop short of explicitly defining barriers. The explicit representation of barriers is a step towards defining a semantics of

[2] Descriptive arguments can be considered as informal arguments in contrast to more quantitative, numeric arguments.

safety arguments and allows analysts to reflect on the hazards being mitigated and the associated implications for design and implementation of safe systems so that risk reduction techniques can be more effectively implemented.

In Sections 4 and 5, two existing hazard analyses will be examined and the explicit barriers inherent in the analysis identified. Barrier implications are drawn out and areas of concern for both the hazard analysis and any associated design are highlighted. The case studies are the proposed design of a computer-aided detection tool (CADT) for mammography and the feasibility of eight-state free route airspace.

4 Computer-aided mammography example

The UK Breast Screening Programme is a national service that involves a number of screening clinics, each with two or more radiologists. Initial screening tests are by mammography, where one or more X-ray films (mammograms) are taken by a radiographer. Each mammogram is then examined for evidence of abnormality by two experienced radiologists [8]. A decision is then made as to whether to recall a patient for further tests because there is suspicion of cancer [23]. Within the screening process it is desirable to achieve the minimum number of false positives (FPs), so that fewer women are recalled for further tests unnecessarily, and the maximum true positive (TP) rate, so that few cancers will be missed [8]. Unfortunately the radiologists' task is a difficult one because the small number of cancers is hidden among a large number of normal cases. Also the use of two experienced radiologists, for *double readings*, makes this process labour intensive.

Computer-based image analysis techniques are being explored to enable a single radiologist to achieve performance that is equivalent or similar to that achieved by double readings [2, 8]. Computer-aided detection systems can provide radiologists with a useful "second opinion" [24]. The case study in this section involves the introduction of a CADT as an aid in screening mammograms. When a CADT is used, the radiologist initially views the mammogram and records a recall decision. The CADT marks a digitised version of the X-ray film with "prompts" that the radiologist should examine. The proposed procedure is that the radiologist records a decision before looking at the CADT prompted x-ray film. A final decision on a patient's recall is then taken by the human radiologist based on the original decision and the examination of the marked-up X-ray. A summary of this process can be seen in Figure 1 (from [23]).

A system based on the model shown in Figure 1 has been investigated to identify the undesirable consequences that may arise. An incorrect recall decision resulting from a misdiagnosis of cancer is an example of such an consequence. The general argument for safe use involves a number of argument legs covering three main activities namely (i) human analysis of the X-ray, (ii) CADT analysis of the X-ray and (iii) the recall decision by the human, based on a review of their original analysis and the CADT analysis. A HAZOP [12] style analysis for the system was completed by a team including the authors [21]. HAZOP is described as a technique of *imaginative anticipation* of hazards and operation

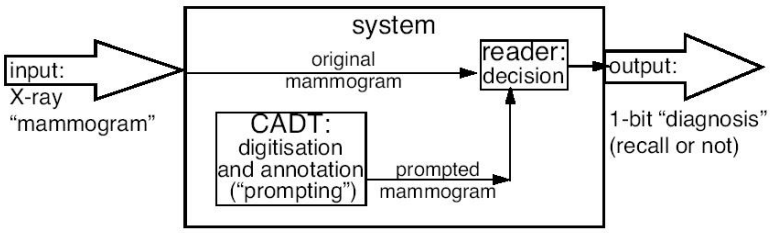

Fig. 1. Model for person using computerised aid for reading mammograms in breast screening.

problems [16, pg43]. It is a systematic technique that attempts to consider events in a system or process exhaustively. The output from this process was a HAZOP table summarising cause, consequence and protection relations to hazards identified in the proposed system (see Table 3 in Appendix A for four example HAZOP rows).

The CADT HAZOP contained 105 HAZOP rows and 61 hazards that required mitigation. In total 99 barriers were identified in the mitigation arguments of the 61 identified hazards. Typical implied barriers included human oriented barriers such as "staff training", environmental conditions, for example "room layout", and system components, for example "bar codes on x-rays". The barriers were identified through the examination of the mitigation arguments present in the HAZOP. Each barrier was considered independent as validating true independence between the associated mitigation arguments is non-trivial and outside the scope of this paper. By examining these barriers further insight into the implications of the hazard mitigation can be derived in the context of the proposed system. The following sections present several views on the nature of barriers identified in post HAZOP analysis. However, it should be noted that these are not necessarily an exhaustive set of the barrier properties or implications for safety.

4.1 Preventive vs. protective barriers

It is common for hazard mitigations to be considered in terms of independence and diversity. The belief that a hazard has been mitigated may be given a higher level of confidence if multiple diverse arguments are present. Also the nature of the associated barrier in the context of the initiating hazard event is also of relevance. Classifying preventive and protective barriers highlights this consideration. For example if a hazard has only preventive barriers there is no fault tolerance in the system, as provided by protective barriers.

In the mammography analysis there are 7 examples of protective barriers and 92 examples of preventive barriers. Two of the protective barriers and 15 of the preventive barriers are unique. Therefore the majority of the barrier protection in this system is based on preventive barriers. This has implications for the

fault tolerance of the system as the failure of preventive barriers may lead to a potentially hazardous system state not anticipated by the designers.

4.2 Barrier frequency and type

Commonly there is not a one-to-one relation between hazards and barriers. One hazard may be protected against by several barriers (see Section 4.3) and one barrier may feature in the mitigation arguments of several hazards. A barrier mitigation with a number of high consequence hazards will require greater reliability as more of the system safety will be dependent on it. This is particularly the case if a single barrier is the only defence to a hazard (see Section 4.3). In addition there may be cost-benefit tradeoffs between barriers. Expensive barriers, in terms of physical cost, time to implement and/or ongoing maintenance, that provide protection against a single hazard may be less desirable than alternative barrier solutions that provide protection from multiple hazards. Such knowledge can provide justification for particular design decisions.

Table 1. Eight most common barriers in the mammography analysis

Barrier	*Frequency*	*Barrier*	*Frequency*
Staff training	23	Good practice following	19
CADT reliability	12	Timetable enforcement	7
Safety culture	6	Bar codes on x-rays	6
User experience	6	CADT testing	5

Table 1 shows the eight most common barriers in the mammography analysis. The top two most common barriers are human oriented and together contribute 42% of the barriers for this example. This may seem surprising considering this system is a technology based solution to a labour intensive process. Even in this computer-based system there is reliance on appropriate training in the mitigation of hazards. Also these human oriented barriers operate when the system is live and are therefore prone to performance variation and other human-error issues (see [17]). Technology based barriers, e.g. "CADT reliability", "bar codes on x-rays" and "CADT testing", contribute 23% of the barriers. From a total of 17 unique barriers identified in the hazard analysis, barriers in the top eight represent 85% of the total barriers. Identifying the barriers that have the most impact can allow developers to focus their efforts.

In addition to the occurrence of particular barriers in this case study, the frequency of demand of barriers significantly modifies the predicted risk. Expectations on how often a barrier will be expected to be active, and not fail, will determine how critical it is to the system it is protecting. However, the analysis material discussed in this paper does not provide details of such expectations and will therefore not be discussed here further.

4.3 Barriers per hazard

Accidents happen because barriers fail and hazards are present. Hollnagel [9] observes that accidents are frequently characterised in terms of the events and conditions that led to the final outcome or in terms of the barriers that have failed. As a consequence, redundancy is a common feature in the safety aspects of dependable systems. In particular, redundancy is used to prevent the failure of a single component causing the failure of a complete system - a so-called *single-point failure* [22, pg 132]. Identifying potential single-point failures is essential for determining problem areas in a system's reliability. Hazards with only single barriers, and in particular single preventive barriers, represent a significant threat to system safety. In addition, identifying multiple barriers does not necessarily imply greater prevention or tolerance properties. Barrier interdependence will compromise any diversity based arguments if combined dependability between barriers results in single-point failure situations. A common preventive barrier pair in the mammography example is the use of "staff training" and "good procedure following" which are clearly interrelated.

In the mammography analysis 33 hazards are protected against by single barriers, 14 hazards by double barriers, 12 hazards by triple barriers and 2 hazards by quadruple barriers. Therefore 54% of the barriers in this analysis suffer from potential single-point failures. Of the single-point failure barriers 5 are protective barriers and 29 are preventive barriers. This reinforces the barrier bias demonstrated in Section 4.1. In this case the additional 2 protective barriers examples are double barriers with, the same, one protective ("bar codes on x-ray") and one preventive ("good procedure following") barrier each. In this case independence can be observed informally between a technology based barrier and a human oriented barrier. There is a need to determine such independence if accurate predictions of barrier performance are to be generated.

5 Airspace route feasibility example

Eurocontrol's European Air Traffic Management Programme requires a safety assessment to be performed for "all new systems and changes to existing systems."[5]. Therefore a safety assessment was commissioned for the eight-states[3] free route airspace concept. The overriding aim of the concept was to obtain benefits in terms of safety, capacity, flexibility and flight efficiency by removing the constraints imposed by the fixed route structure and by optimising the use of more airspace [6, pg xiii]. The principal safety objective was to ensure that free route airspace operations are at least as safe as the current fixed route operations. A functional hazard assessment was completed to determine how safe the various functions of the system need to be in order to satisfy the safety policy requirements. This assessment investigated each function of the proposed system and identified ways in which it could fail (i.e. the hazards) [6, pg 10].

[3] Belgium, Denmark, Finland, Germany, Luxembourg, The Netherlands, Norway and Sweden.

This hazard assessment has been examined in a similar manner to that described in Section 4 (see Table 4 in Appendix A for three example hazard assessment rows). Although the two cases are not directly comparable, examining the explicit barriers present in the airspace route provides insight into the identification of barriers as both a design tool and possible analysis metric. Analysis is based on the mitigations associated with the new hazards introduced by the implementation of free route operations and ignores existing mitigations in the previous system.

The functional hazard assessment contains 105 rows of which 69 contained new hazards that required mitigation. Newly identified hazards are not mitigated by existing mitigating factors in the system. The output of the hazard assessment was a set of safety requirements for the proposed free route environment. In total 128 barriers can be identified in the safety requirements. For example assessment 210 in Table 4 of Appendix A contains four existing mitigating factors and four proposed barriers described as safety requirements. Other implied barriers in this case study include human oriented barriers such as "controller training", environmental conditions, for example "airspace design", and system components, for example "MTCD[4] system usage". The following sections are indicative of the set of barrier properties and of their implications for safety.

5.1 Preventive vs. protective barriers

No protective barriers and 128 preventive barriers were identified in the free route airspace example. The majority consist of the enforcement or review of different operating procedures. Other barriers include controller and pilot training and monitoring system technology. Twenty two different preventive barriers can be identified as unique barrier forms. All of the barrier protection is based on preventive barriers here, which has implications for the fault tolerance of the system.

5.2 Barrier frequency and type

Table 2 shows the eight most common barriers in the airspace analysis. The two barriers that appear most common in the hazard analysis are technological systems and together contribute 39% of the barriers. In Table 2 technological systems represent 48% of the total barriers and the human oriented barriers represent 24%. From a total of 22 unique barriers identified in the analysis, those in Table 2 represent 84% of all the barriers in this hazard analysis.

5.3 Barriers per hazard

In this analysis 28 hazards are protected against by single barriers, 31 hazards by double barriers, 10 hazards by triple barriers and 3 hazards by quadruple barriers. Therefore 22% of the barriers in this analysis suffer from potential

[4] Medium Term Conflict Detection.

Table 2. Eight most common barriers in the airspace analysis

Barrier	*Frequency*	*Barrier*	*Frequency*
MONA (MONitoring Aid) system	32	MTCD system	18
Controller training	18	Free Route Airspace contingency procedures	15
Airspace design	8	Review procedures	8
Transfer procedure	5	Area Proximity Warning (APW) system	4

single-point failures. Although this is less than in the CADT for mammography example it represents a considerably percentage of the barriers proposed in this assessment. As with the CADT analysis (see Section 4), each barrier was considered independent and determining independence between barriers is outside the scope of this paper.

6 Explicit barriers for certification

Storey [22] notes three typical aspects to the certification of safety-critical systems:

1. A demonstration that all important hazards have been identified and dealt with, and that the integrity of the system is appropriate for the application.
2. Evidence of compliance with some particular standard.
3. A rigorous argument to support the claim that the system is sufficiently safe and will remain so throughout its life.

Explicit barrier definition through the development phases of a safety-critical system form a traceable hazard mitigation link in the associated documentation. Barriers identified via hazard analysis will require representation in any design rationale and associated safety case used to assure system safety. In addition whether hazard mitigations, as represented by abstract barriers in a design, are in fact present and functioning in a live system can be determined. Therefore the explicit representation of barriers highlights the hazard mitigations that are in place and their continuing performance.

There is little information on final implementation and performance of the case studies described in this paper. However, they can be examined in the context of the proposed designs. This allows designers to reflect on the identified barriers and their influence on any future certification.

User training as a preventive barrier has played a considerable part in the mitigation of hazards in both the CADT for mammography and the free route airspace examples. Verification that appropriately qualified staff are part of the human-machine system would therefore be required. This may require the introduction of additional barriers, such as qualification checking, confirmation of accreditation of training schemes and continuous assessment of actual performance.

The majority of barriers in the free route airspace example were based on the development and implementation of future products, for example, the review and definition of good operating procedures in particularly hazardous situations and the deployment of proposed traffic monitoring technology. It is likely that these barriers would feature predominantly in any safety case based in part on this hazard assessment. Verification of the existence of these procedures and their acceptance in the organisational structure of the domain would be required. Also the barriers indicating the use of the new traffic monitoring technology (MONA) provides a minimum level of functionality for the deployed system. Therefore the performance between any predicted barrier behaviour, commonly presented as evidence as part of a safety case, and the actual barrier behaviour in the live system can provide a quantitative measure of barrier reliability for certification purposes.

7 Conclusions

Barriers are important for the understanding and prevention of accidents and are an intrinsic part of safety-critical systems. They feature implicitly throughout a system's development life-cycle. In additional to having physical presense in a live system, they provide a representation for safety concerns in hazard analysis, design decisions, safety case construction and certification.

In this paper several views on the explicit representation of barriers have been presented. These aid the understanding of hazards as represented in the analysis of safety-critical systems. Reflecting on the choice and nature of barriers is an essential part of constructing more dependable systems. Two case studies have been examined and the implication of barriers in the context of a hazard analysis have been defined. The process of hazard mitigation in a design can be documented by considering barriers explicitly. In addition, this process provides a framework for a quantitative measure of barriers as part of the certification process.

Analysing and defining barrier descriptions is a time consuming process which would be aided considerably by a barrier notation and tool support. The authors are currently investigating the use of the Hazard-Barrier-Target model [18] and the Safety Modelling Language [19] as the next step to incorporating explicit barriers in safety-critical system development. This is ongoing work.

8 Acknowledgements

This work was supported in part by the UK EPSRC DIRC project [4], GR/N13999 and by the ADVISES research training network, GR/N 006R02527.

References

1. Stephen Barker, Ian Kendall, and Anthony Darlison. Safety cases for software-intensive systems: an industrial experience report. In Peter Daniel, editor, *16th*

International Conference on Computer Safety, Reliability and Security (SAFECOMP 97), pages 332–342. Springer, 1997.

2. Caroline R. M. Boggis and Susan M. Astley. Computer-assisted mammographic imaging. *Breast Cancer Research*, 2(6):392–395, 2000.
3. B. S. Dhillon. Failure modes and effects analysis - bibliography. *Microelectronics and Reliability*, 32(5):719–731, 1992.
4. DIRC - Interdisciplinary Research Collaboration on Dependability of Computer-Based Systems, http://www.dirc.org.uk [last access 6/06/2003], 2003.
5. European air traffic management programme safety policy, November 1995. SAF.ET1.ST01.1000-POL-01-00, Edition 1.0.
6. Eurocontrol. Safety assessment of the free route airspace concept: Feasibility phase. Working Draft 0.3, European Organisation for the Safety of Air Navigation, October 2001. 8-States Free Route Airspace Project.
7. Lars Harms-Ringdahl. Investigation of barriers and safety functions related to accidents. In *Proceedings of the European Safety and Reliability Conference ESREL 2003*, Maastricht, The Netherlands, 2003.
8. Mark Hartswood and Rob Proctor. Computer-aided mammography: A case study of error management in a skilled decision-making task. In Chris Johnson, editor, *Proceedings of the first workshop on Human Error and Clinical Systems (HECS'99)*. University of Glasgow, April 1999. Glasgow Accident Analysis Group Technical Report G99-1.
9. Erik Hollnagel. Accidents and barriers. In J-M Hoc, P Millot, E Hollnagel, and P. C. Cacciabue, editors, *Proceedings of Lex Valenciennes*, volume 28, pages 175–182. Presses Universitaires de Valenciennes, 1999.
10. C. W. Johnson. *Failure in Safety-Critical Systems: A Handbook of Accident and Incient Reporting*. University of Glasgow Press: Glasgow, Scotland, October 2003. ISBN 0-85261-784-4.
11. T. P. Kelly, I. J. Bate, J. A. McDermid, and A. Burns. Building a preliminary safety case: An example from aerospace. In *1997 Australian Workshop of Industrial Experience with Safety Critical Systems*, Sydney, Australia, 1997. ACS.
12. Trevor Kletz. *Hazop and Hazan: Identifying and Assessing Process Industrial Hazards*. Institution of Chemical Engineers, third edition, 1992. ISBN 0-85295-285-6.
13. Nancy G. Leveson. *Safeware: System Safety and Computers*. Addison Wesley, 1995.
14. P. Neogy, A. L. Hanson, P. R. Davis, and T. E. Fenstermacher. Hazard and barrier analysis guidance document. Technical Report EH-33, Department of Engery, Office of Operating Experience Analysis and Feedback, USA, November 1996. Rev 0.
15. Steven Pocock, Michael Harrison, Peter Wright, and Paul Johnson. THEA - a technique for human error assessment early in design. In Michitaka Hirose, editor, *Human-Computer Interaction: INTERACT'01*, pages 247–254. IOS Press, 2001.
16. David. J. Pumfrey. *The Principled Design of Computer System Safety Analysis*. PhD thesis, Department of Computer Science, The University of York, 2000.
17. James Reason. *Human Error*. Cambridge University Press, Cambridge, 1990.
18. Bastiaan A. Schupp, Saul M. Lemkowitz, and Hans J. Pasman. Application of the Hazard-Barrier-Target (HBT) model for more effective design for safety in a computer-based technology management environment. In *CCPS ICW: Making Process Safety Pay: The Business Case*, pages 287–316. AIChE/CCPS, 2001.
19. Bastiaan A. Schupp, Shamus P. Smith, Peter C. Wright, and Louis H. J. Goossens. Integrating human factors in the design of safety critical systems: A barrier based

approach. In *Proceedings of IFIP 13.5 Working Conference on Human Error, Safety and Systems Development (HESSD 2004)*. Forthcoming, 2004.
20. Shamus P. Smith and Michael D. Harrison. Improving hazard classification through the reuse of descriptive arguments. In Cristina Gacek, editor, *Software Reuse: Methods, Techniques, and Tools (ICSR-7)*, volume 2319 of *Lecture Notes in Computer Science (LNCS)*, pages 255–268, Berlin, 2002. Springer.
21. Shamus P. Smith and Michael D. Harrison. Reuse in hazard analysis: Identification and support. In Stuart Anderson, Massimo Felici, and Bev Littlewood, editors, *Computer Safety, Reliability and Security (SAFECOMP 2003)*, volume 2788 of *Lecture Notes in Computer Science (LNCS)*, pages 382–395, Berlin, 2003. Springer.
22. Neil Storey. *Safety-Critical Computer Systems*. Addison-Wesley, 1996.
23. L. Strigini, A. Povyakalo, and E. Alberdi. Human-machine diversity in the use of computerised advisory systems: a case study. In *IEEE International Conference on Dependable Systems and Networks (DSN 2003)*, pages 249–258. IEEE, 2003. San Francisco, U.S.A.
24. Bin Zheng, Ratan Shah, Luisa Wallance, Christiane Hakim, Marie A. Ganott, and David Gur. Computer-aided detection in mammography: An assessment of performance on current and prior images. *Academic Radiology*, 9(11):1245–1250, November 2002. AUR.

A Raw hazard analysis fragments

Table 3. Fragment of HAZOP for the CADT for mammography design

Ref	Item	Guideword	Cause	Consequence/Implication	Indication/Protection
1.1.1a	Make initial decision	Wrong	Radiologist inexperience	Wrong detection result	Training
...					
1.1.1.1g	Examine x-ray	Repeat	X-rays out of order	Mixed up detection and patient record	Barcoding on x-ray and patient record. Srict procedure
...					
1.2a	Process digital x-ray	Omit	System failure	No CADT image. Reliance on human decision	CADT reliability
...					
1.3.3a	Record decision	Omit	Operator lapse	Loss of records	Interlock to force form completion

Table 4. Fragment of safety assessment for the free route airspace concept

Task	Function	ID	Failure Condition	Operational Consequences	Existing mitigating factors	Proposed Free Route safety requirement
Handling aircraft	Conflict identification	210	Controller fails to identify conflict	Potential collision risk	Controller training. Pilot awareness of other traffic. STCA[b], TCAS[c]	MTCD[a]. Controller training. Airspace design. Procedure review.
Handling aircraft	Conflict identification	211	Controller unable to make timely identification of conflict	Potential collision risk	Controller training. Pilot awareness of other traffic STCA, TCAS.	MTCD. Airspace design. Controller training. Transfer procedures
Handling aircraft	Conflict identification	212	Controller mistakenly identifies conflict when none existed	Extra workload	Controller training. Traffic monitoring	MTCD. Controller training.

[a] Medium Term Conflict Detection system.
[b] Short Term Conflict Alert system.
[c] Traffic Alert Collision Avoidance System.